

Universidad de Huánuco

Facultad de Ingeniería

ESCUELA ACADÉMICO PROFESIONAL DE INGENIERÍA DE SISTEMAS E INFORMÁTICA



TESIS

PENTESTING VOIP PARA DETERMINAR LAS
VULNERABILIDADES DEL SERVIDOR DE COMUNICACION
DEL AREA DE SOPORTE DE LA EMPRESA CHAPACUETE
DE LA CIUDAD DE HUÁNUCO PERIODO 2019.

Para Optar el Título Profesional de:
INGENIERO DE SISTEMAS E INFORMÁTICA

TESISTA

MARTEL RAMOS Ivan Cruz

ASESOR

Mg. JACHA ROJAS, Johnny Prudencio

Huánuco - Perú
2019



UNIVERSIDAD DE HUANUCO
Facultad de Ingeniería

E.A.P. DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

**ACTA DE SUSTENTACIÓN DE TESIS PARA OPTAR EL TÍTULO
PROFESIONAL DE INGENIERO (A) DE SISTEMAS E INFORMÁTICA**

En la ciudad de Huánuco, siendo las 18:00 horas del día 18 del mes de noviembre del año 2019, en el Auditorio de la Facultad de Ingeniería, en cumplimiento de lo señalado en el Reglamento de Grados y Títulos de la Universidad de Huánuco, se reunieron el **Jurado Calificador** integrado por los docentes:

Mtro. Walter Baldeón Canchaya..... (Presidente)
Mtro. Fabio Rodríguez Meléndez..... (Secretario)
Mtro. José Núñez Vicente..... (Vocal)

Nombrados mediante la Resolución N° 1309-2019-D-FI-V04, para evaluar la Tesis intitulada:

"Pentesting VOIP para determinar las vulnerabilidades del servidor de comunicación del área de soporte de la empresa CHAPACETE de la ciudad de Huánuco periodo 2019....."
....., presentado por el (la) Bachiller Juan Cruz Martel Ramos....., para optar el Título Profesional de Ingeniero (a) de Sistemas e Informática.

Dicho acto de sustentación se desarrolló en dos etapas: exposición y absolución de preguntas; procediéndose luego a la evaluación por parte de los miembros del Jurado.

Habiendo absuelto las objeciones que le fueron formuladas por los miembros del Jurado y de conformidad con las respectivas disposiciones reglamentarias, procedieron a deliberar y calificar, declarándolo (a) Aprobado por Unanimidad con el calificativo cuantitativo de 14 y cualitativo de Suficiente (Art 47)

Siendo las 19:10 horas del día 18 del mes de noviembre del año 2019, los miembros del Jurado Calificador firman la presente Acta en señal de conformidad.


Presidente


Secretario


Vocal

DEDICATORIA

La presente tesis está dedicada a Dios, ya que gracias a él he logrado concluir mi carrera.

A mis padres, porque todo lo que soy se lo debo a ellos y por estar siempre a mi lado brindándome su apoyo, sus consejos para hacer de mí una mejor persona y por inculcar en mí la importancia de estudiar.

AGRADECIMIENTO

Este trabajo es dedicado a todos los involucrados en brindar conocimiento, sus experiencias y tiempo, que hacen crecer día a día una sociedad más responsable.

INDICE

DEDICATORIA	II
AGRADECIMIENTO	III
INDICE.....	IV
RESUMEN.....	VI
ABSTRACT	VII
INTRODUCCIÓN	VIII

CAPÍTULO I

LINEA DE INVESTIGACIÓN

1.1. Descripción de la línea de investigación	9
1.2. Descripción del Problema	9
1.3. Justificación del Problema.....	10
1.3.2. Propuesta de Solución y Alcance	10
1.4. Objetivo Principal.....	11
1.5. Objetivos Secundarios	11

CAPÍTULO II

MARCO TEÓRICO

2.1 Antecedentes de la investigación	13
2.2 Definiciones conceptuales	18

CAPITULO III

METODOLOGIA DE LA INVESTIGACIÓN

3.1	Metodología de la investigación	23
3.2	Herramientas	27

CAPÍTULO IV

DESARROLLO E IMPLEMENTACION

4.1.	Desarrollo e Implementación	30
4.2.	Pruebas.....	39
CONCLUSIONES		43
REFERENCIAS BIBLOGRÁFICAS		44

RESUMEN

La investigación se enfocó que en análisis de las vulnerabilidades del servidor VOIP de la empresa Chapacuate de la ciudad de Huánuco. El proceso de pentesting consistió en la aplicación de una serie de herramientas bajo software libre para la determinación de vulnerabilidades del servidor de telefonía bajo el sistema operativo GNU/Linux usando la distribución Asterisk. Se realizaron pruebas de ataque usando técnicas como Man In The Middle y ARP spoofing, y se llegaron a descubrir una serie de vulnerabilidades como por ejemplo: puertos abiertos en el servidor, servicios innecesarios habilitados, contraseña del root débil, extensiones con la configuración por defecto, y la vulnerabilidad más importante fue que en el servidor se estaba utilizando como protocolo de comunicación a SIP un protocolo con muchas vulnerabilidad en relación al cifrado de la comunicación.

Se pudo advertir a tiempo y corregir las vulnerabilidades, como por ejemplo de utilizar el protocolo IAX para mejorar la seguridad en cuanto al transporte de las comunicaciones por la red de datos. Las pruebas se realizaron en diferentes escenarios, tanto virtual como físico, así mismo se implementó un cronograma de pruebas para llevar a cabo la aplicación de estas herramientas y determinar el proceso o la repetición de las vulnerabilidades en el servidor. En la fase de ataque se simuló un agente en la cual se asumió un cliente conectado a la red para interceptar las llamadas realizadas por los usuarios, con las herramientas específicas se pudo obtener dichas llamadas y guardarlas como archivo para su posterior análisis.

Palabras clave: VOIP, VOIP pentesting, ethical hacking, asterisk.

ABSTRACT

The investigation focused on the vulnerability analysis of the VOIP server of the Chapacuate company of the city of Huánuco. The process of pentesting consisted in the application of a series of tools under free software for the determination of vulnerabilities of the telephony server under the GNU / Linux operating system using the Asterisk distribution. Attack tests were performed using techniques such as Man In The Middle and ARP spoofing, and a number of vulnerabilities were discovered such as: open ports on the server, unnecessary services enabled, weak root password, extensions with default settings , and the most important vulnerability was that a protocol with a lot of vulnerability regarding communication encryption was being used as the SIP communication protocol. It was possible to warn in time and correct vulnerabilities, such as using the IAX protocol to improve security regarding the transport of communications over the data network. The tests were carried out in different scenarios, both virtual and physical, and a test schedule was implemented to carry out the application of these tools and determine the process or the repetition of vulnerabilities in the server. In the attack phase an agent was simulated in which a client connected to the network was assumed to intercept the calls made by the users, with the specific tools it was possible to obtain said calls and save them as a file for later analysis.

Keywords: VOIP, VOIP pentesting, ethical hacking, asterisk.

INTRODUCCIÓN

La investigación se desarrolló bajo la metodología de la investigación basada en proyectos tecnológicos, consistiendo en la aplicación de pruebas de vulnerabilidades del servidor de telefonía de la empresa Chapacuate de la ciudad de Huánuco. La metodología que se empleó: PTES (Penetration Testing Execution Standart) que consta de siete secciones principales: recolección de información, análisis de vulnerabilidades, explotación, post-explotación e informes. Como objetivos secundarios se consideró: Virtualizar los entornos de red, tanto el servidor de comunicación como los clientes, ejecutar la fase de reconocimiento y clasificar la información obtenida, realizar la fase de penetración, donde se realizan las pruebas y los ataques correspondientes, explotar el sistema y listar las vulnerabilidades, proponer las alternativas de solución y documentar el proceso de prueba.

Siendo una investigación tecnológica, se utilizaron los propios instrumentos de medición incluidos en las herramientas software, y para la representación de los resultados se usaron algunos cuadros, cabe destacar que la fase de penetración fue la que más se realizó ya que los resultados entre una y otra toma variaban, así que se llegó a estandarizar y promediar los resultados obtenidos por cada prueba.

Al finalizar la investigación se concluyó que la vulnerabilidad más crucial fue la del uso del protocolo SIP, siendo este último un protocolo desfasado y con deficiencias en el tema de la seguridad, por ende después de las pruebas se optó por reemplazarlo por el protocolo IAX, que permitió que las comunicaciones fueran cifradas evitando el famoso chuponeo o interceptación de llamadas.

CAPÍTULO I

LINEA DE INVESTIGACIÓN

1.1. Descripción de la línea de investigación

La investigación esta inmersa dentro de la política: Seguridad Informática, bajo la línea de investigación: Seguridad Informática, cuya referencia es: Busca analizar, desarrollar e implementar herramientas y técnicas para preservar la confidencialidad, integridad y disponibilidad de la información digital.

1.2. Descripción del Problema

La información como activo en una organización, es pieza clave en el desarrollo y evolución de la misma, con la información se llegan a tomar buenas decisiones y a tiempo, es por eso que hoy en día las empresas le asignan un valor único y diferenciado dentro de los activos de la organización. Las empresas invierten en la protección de la información que poseen, la seguridad informática cumple con velar la confidencialidad, integridad y disponibilidad de la información. Es así que en la empresa Chapacuate ubicada en la Av. Colectora Mz. G Lote. 3 y con su fabrica instalada en la provincia de Ambo, cuenta con varias áreas y gestiona información para cada una de estas, para el cumplimiento de sus objetivos empresariales, así como la misión y visión trazada. La empresa cuenta con un servidor de telefonía IP, para dar el servicio de llamadas telefónicas y grabaciones mediante el uso de una red de datos. Dicha red ha sido vulnerada en varias ocasiones, estos sucesos fueron registrados y reportados a la misma gerencia: algunos trabajadores contratados y/o practicantes del área de sistemas, han venido realizando pruebas de penetración de la red de telefonía IP y realizando escuchas y grabaciones no autorizadas de la diferentes áreas de la empresa, esto ha causado preocupación por parte de la gerencia ya que el temor es la fuga de

información hacia otras empresa del rubro y así como también violar la confidencialidad de las llamadas dentro de la organización.

En base a lo descrito en los párrafos anteriores, se ha planteado una solución a dicho problema usando técnicas de pentesting o pruebas de funcionamiento y detección de vulnerabilidades del servidor de telefonía IP, usando los ataques arp spoofing y Eavesdropping para la escucha de llamadas, así mismo plantear alternativas de solución y de seguridad en la red de telefonía interna.

1.3. Justificación del Problema

1.3.1. Justificación Práctica

Se justifica de una forma práctica esta investigación por el uso de herramientas informáticas que, aplicadas en la práctica, solucionarían el problema de carencia de confidencialidad en la red de telefonía de la empresa Chapacuate de la ciudad de Huánuco.

Justificación Teórica

Con la aplicación y resultados de la investigación, esta dotará a la comunidad informática de la localidad una propuesta de mejora donde se describirá a detalle la técnicas, procedimientos de forma grafica y explicada de como asegurar la confidencialidad en una red de Telefonía VOIP, dado que en la revisiones de Tesis a nivel local y nacional se cuenta con una información mínima y no especializada.

1.3.2. Propuesta de Solución y Alcance

La investigación se enfoca en la prueba de penetración o Pentesting a la red de telefonía VOIP de la empresa Chapacuate, para determinar las vulnerabilidades que presenta y así mismo corregirlas, para posteriormente elaborar una guía documentada de las actividades realizadas.

La propuesta de solución se muestra en el siguiente gráfico:



La solución empieza con la recopilación y clasificación de información de la red de telefonía, luego el estudio y análisis de la misma, pasando por la identificación de los puntos de acceso y de los fallos, para finalmente realizar la evaluación de los riesgos de las vulnerabilidades identificadas.

Posteriormente se elabora la propuesta de solución y documentación de la parte técnica, para así poder ser aplicada en otros entornos donde se use también las distribuciones de software y hardware para el funcionamiento de una red de telefonía VOIP.

El alcance de esta investigación se refleja en la investigación de la red de telefonía VOIP de la red local de datos de la empresa, una prueba de penetración interna mas no externa. Las herramientas a usarse están diseñadas para cumplir una función genérica, lo que el investigador tiene la tarea de adecuarlas al proceso de prueba.

1.4. Objetivo Principal

Ejecutar la prueba de vulnerabilidad – Pentesting al servidor de Telefonía VOIP de la empresa Chapacuate de la ciudad de Huanuco.

1.5. Objetivos Secundarios

- ✓ Virtualizar los entornos de red, tanto el servidor de comunicación como los clientes.
- ✓ Ejecutar la fase de reconocimiento y clasificar la información obtenida.

- ✓ Realizar la fase de penetración, donde se realizan las pruebas y los ataques correspondientes.
- ✓ Explotar el sistema y listar las vulnerabilidades.
- ✓ Proponer las alternativas de solución y aplicarlas
- ✓ Documentar el proceso de prueba.

CAPÍTULO II

MARCO TEÓRICO

2.1 Antecedentes de la investigación

A nivel Internacional

Caceres y Carriel (2017), realizó la investigación: *Análisis De Vulnerabilidades En Los Sistemas De Telefonía IP De La Microempresa Telenetcorp S.A. Utilizando Herramientas De Test De Penetración*. En la Universidad de Guayaquil, Ecuador. La investigación llegó a las siguientes principales conclusiones: La microempresa TELENETCORP S.A. mediante el análisis de vulnerabilidades ha hecho conciencia sobre la protección contra virus y salvaguardar la información de carácter confidencial. Ha considerado la importancia de contar con medidas de seguridad adecuadas y planes de contingencia que ayuden a la protección de la red de telefonía IP ante intrusiones internas y externas. Para salvaguardar la información de carácter confidencial se puede usar el comando Nmap, que permite a la microempresa TELENETCORP S.A. conocer en el sistema de telefonía IP aquellos puertos vulnerables; y, de esta forma poder tomar acciones adecuadas que permitan mitigar riesgos y tenerlos bajo control. Hoy, aquellos profesionales responsables de la seguridad informática se basan en un test de penetración para verificar los riesgos que pueden tener los sistemas de telefonía IP y que tipo de información está expuesta. Con este tipo de análisis se pueden proporcionar diferentes alternativas en seguridad, como la implementación de sistemas de encriptación VPN que garantizan la privacidad de las llamadas y firewalls que tengan políticas de seguridad establecidas para el filtrado de puertos evitando conexiones no autorizadas a la central telefónica. Con la ayuda de sistemas detectores de intrusos, se pueden detectar usuarios maliciosos que intenten tener el acceso a la central de telefonía IP y emitir alarmas para reportar la microempresa TELENETCORP S.A. sobre una intrusión presente.

Calderón (2015), realizó la investigación: *Implementación de protocolos de seguridad para la red VoIP del Hospital Isidro Ayora de Loja*. En la Universidad Nacional de Loja, Ecuador. La investigación llegó a las siguientes principales conclusiones: Con la configuración e implementación del protocolo de seguridad (TLS), en el servidor de Asterisk se contrarrestó ataques como el eavesdropping (MitM), es decir, se redujo drásticamente las escuchas indebidas en la red, ya que (TLS), genera un túnel cifrado para la transmisión de la comunicación entre los dos extremos (origen, destino) y de esta manera proteger la integridad, disponibilidad y confidencialidad de la información. Las soluciones que se implementaron en el archivo sip.conf, tuvieron éxito porque se logró bloquear a usuarios anónimos que intentaban acceder al sistema, con el fin de obtener información del servidor, de esta manera se ha logrado contrastar las vulnerabilidades encontradas, como la (DoS), sin embargo, es importante pensar que estas no son las únicas soluciones posibles y que no habrá medida de seguridad que brinde el 100%, de fiabilidad, pero existen métodos para corregir estas vulnerabilidades, sobre todo, está el sentido común del administrador de la red, para realizar medidas de protección y despistar a los usuarios mal intencionados que quieran ingresar a su sistema. Durante la etapa de análisis y el testing de vulnerabilidades aplicadas a las comunicaciones (VoIP), se demostró que existen amenazas de seguridad, causadas por contar con las configuraciones por defecto del servidor Asterisk, falta de robustez en sus contraseñas o las mismas contraseñas para el acceso a los sistemas, además, se tenía puertos innecesarios abiertos en el servidor los cuales mostraban los servicios que se están corriendo en cada uno de ellos, debido a esto se facilitó la tarea para ingresar de manera anónima al sistema, estas vulnerabilidades se corrigieron con la instalación de la herramienta fail2ban y asegurando el puerto (SSH), del servidor. El uso de herramientas informáticas (sniffer), facilita la tarea del investigador para determinar las vulnerabilidades informáticas dentro de una organización se logró. determinar que el servidor de comunicaciones (VoIP) del Hospital estaba sujeto a vulnerabilidades con un alto riesgo de probabilidad, como son las escuchas indebidas en la red (eavesdropping). Con la configuración de los

parámetros de seguridad en el archivo `sshd_config`, se demostró que se reduce potencialmente el acceso al sistema, ya que a que se asigna permisos únicos para administrados de la red, autenticándose únicamente por un clave privada, con esto estamos bloqueando a usuarios mal intencionados que intenten ingresar al sistema, por lo tanto se reduce al mínimo las vulnerabilidades de cracking de contraseñas y accesos no autorizados. Los problemas de seguridad en redes (VoIP) no solo radican en los protocolos en los que se apoyan para generar los servicios de telefonía. Hay que tener muy en cuenta la seguridad de la red de datos por las que se trasmite, debido a que la tecnología (VoIP) hereda las vulnerabilidades de una red de datos tradicional. Los procesos de la metodología (OCTAVE) permiten llevar a cabo un proceso minucioso y sistemático,, mientras que la metodología (OSSTMM) dice como se tiene que realizar una evaluación de seguridad, razón por la cual resulta satisfactorio la fusión de estas dos tecnologías, ya que juntas permiten realizar una evaluación completa a los activos de una organización. Por medio de estas metodologías se conoció los puntos críticos en la red (VoIP) y se supo cómo evaluarlos, de esta forma se determinó la probabilidad de amenazas y los ataques a los que están sujetos estos activos, luego se los clasifica de acuerdo a la magnitud e impacto; los riesgos más altos son utilizados para determinar una estrategia de seguridad cuyo fin es contrarrestar dicha vulnerabilidad y evitar ataques que puedan degradar el servicio de la tecnología (VoIP) y por ende el funcionamiento dela institución.

A nivel Nacional

Cruz (2014), realizo la investigación: *Aplicación De Auditoría Penetration Testing Para Contribuir Con La Seguridad De La Información En Los Sistemas Informáticos De La Empresa Data Business SAC, Trujillo*”. En la Universidad Privada del Norte, Trujillo. La investigación lIego a las siguientes principales conclusiones: Con la presente auditoria Penetration

Testing se pudo contribuir a la seguridad de la información en los sistemas informáticos de la empresa DATA BUSINESS SAC, Trujillo. Al identificar 05 vulnerabilidades existentes de calificación ALTA por causas de puertos abiertos (135, 443, 445) y 02 vulnerabilidades por ataques DoS. Trayendo consecuencia de un control parcial de las PC vulneradas. Se pudo identificar a través de la auditoria Penetration Testing el impacto de un fallo de seguridad, que perjudicaría directamente a la Integridad de la información en un 40% del daño ocurrido, así como un 26% a la Integridad de la Información y un 34% a la disponibilidad de la información. El impacto de esta penetración llevó al control parcial de los sistemas de información por parte del atacante a la empresa de Data Business, Trujillo, y a la vez la posibilidad de obtener una gran cantidad de información sobre ellos, incluyendo contraseñas de acceso al servidor, carpetas compartidas, información de correos y todo mediante la explotación de puertos vulnerables. Es Por ello que podemos afirmar que se cumplieron los objetivos de la prueba de penetración. Se propuso alineamientos necesarios que contribuyen a tener controles de seguridad informática cuya información se da a conocer en el informe START, además se recomendó capacitaciones, al observar que el personal no cuenta con la información mínima sobre seguridad informática al poder aplicar Ingeniería Social en ellos. Ignorancia que fue aprovechada por el auditor para realizar las diferentes técnicas de ataque. Se determinó que un atacante remoto sería capaz de penetrar las defensas de Data Business SAC, Trujillo. Para que esta situación se lleve a cabo, el vector de ataque inicial fue de una Denegación de servicio (DoS) aplicado con ingeniería social para engañar a la víctima a favor del atacante y obtener acceso a la red LAN de la empresa, posterior realizar un escaneo de las PC activas y hacer un análisis de sus vulnerabilidades, creando esta una situación de ataque, adicionalmente fue inyectando código malicioso (trojanos y Backdoor) para una conexión específica a distancia (conexión remota). Esto expone a la empresa a un ataque directo con escalada de ataque a la sede principal (granja de servidores) y demás sucursales, que podría conducir a un impacto financiero. La confianza de la empresa Data Business SAC, se vería afectada negativamente si tal evento ocurriera. Fue posible obtener

un control completo sobre las PC de la sede Trujillo. Esto proporcionó al atacante la capacidad de robar información confidencial de clientes, costos y precios de productos, etc., haciendo de este ataque muy perjudicial y muy atractivo para otras empresas del mismo rubro.

Reynosa (2017), realizó la investigación: *Diseño De Un Sistema De Seguridad En La Empresa Mylcom Contra La Intrusión Utilizando Alarma Y Aviso De Alerta Vía VoiP*". En la Universidad de Ciencias y Humanidades, Lima. La investigación llegó a las siguientes principales conclusiones: Al analizar el problema existente en el sistema de seguridad contra la intrusión, este termina con el funcionamiento vía script enlazado entre un microcontrolador y un servidor Asterisk. La labor principal de este sistema de seguridad consiste principalmente en reducir la carga de trabajo de los responsables de seguridad, reducir los costos y agregar un valor agregado al servicio de seguridad de la empresa, fortaleciendo de esa manera la seguridad global de cualquier infraestructura y la calidad del servicio prestado. Existen muchos modelos de seguridad contra la intrusión, sin embargo, el sistema descrito en la presente Tesis ofrece aprovechar que el cliente cuenta con una PBX, implementando un circuito que permita un sistema de vigilancia y que envía a la brevedad un aviso de alerta a través de la red. El principal beneficio de este diseño es para la empresa que a base de deficiencias en seguridad desea implementar sin hacer gastos excesivos y aprovechar su sistema de red, mejorando su servicio y abaratando el proceso de mejora.

A nivel Local

Se hizo la consulta a los repositorios de tesis de las demás universidades de la localidad y no se encontraron trabajos similares.

2.2 Definiciones conceptuales

ARP SPOOFING: Un ARP Spoofing es una especie de ataque en el que un atacante envía mensajes falsificados ARP (Address Resolution Protocol) a una LAN. Como resultado, el atacante vincula su dirección MAC con la dirección IP de un equipo legítimo (o servidor) en la red.

Si el atacante logró vincular su dirección MAC a una dirección IP auténtica, va a empezar a recibir cualquier dato que se puede acceder mediante la dirección IP.

ARP Spoofing permite a los atacantes maliciosos interceptar, modificar o incluso retener datos que están en tránsito. Los ataques de suplantación ARP ocurren en redes de área local que utilizan protocolo de resolución de direcciones (ARP). (Soto, 2016).

CAIN Y ABEL: Caín y Abel es una herramienta de recuperación de contraseñas para los sistemas operativos de Microsoft, se caracteriza por permitir de una forma fácil la recuperación de diversos tipos de contraseñas por diccionario, fuerza bruta, además de permitir sniffear la red en busca de estas contraseñas. (DragonJar, 2018)

EAVESDROPPING: Eavesdropping es la interceptación no autorizada en tiempo real de una comunicación privada, como una llamada telefónica, un mensaje instantáneo, una videoconferencia o una transmisión de fax. El cifrado es una gran defensa contra el eavesdropping . Al usar solo aplicaciones y sistemas que utilizan cifrado fuerte, puede hacer la vida de un atacante mucho más difícil. Pero no es una panacea, por un par de razones:

En primer lugar, continuamos viendo un ataque dual contra datos encriptados. Mientras que las PC siguen la ley de Moore y su velocidad aumenta exponencialmente, las herramientas de seguridad se vuelven más

inteligentes. Las PC más rápidas reducen el tiempo que necesita un atacante para descifrar una contraseña y las tecnologías modernas de descifrado de contraseñas, como las tablas arco iris, pueden revelar las contraseñas en segundos. (Networks, 2018)

IAX: (Inter-Asterisk eXchange protocol) es uno de los protocolos utilizado por Asterisk. Es utilizado para manejar conexiones VoIP entre servidores Asterisk, y entre servidores y clientes que también utilizan protocolo IAX. El protocolo IAX ahora se refiere generalmente al IAX2, la segunda versión del protocolo IAX. El protocolo original ha quedado obsoleto en favor de IAX2.

IAX2 es robusto, lleno de novedades y muy simple en comparación con otros protocolos. Permite manejar una gran cantidad de códecs y un gran número de streams, lo que significa que puede ser utilizado para transportar virtualmente cualquier tipo de dato. Esta capacidad lo hace muy útil para realizar videoconferencias o realizar presentaciones remotas. ESTA DISEÑADO PARA DARLE PRIORIDAD A LOS PAQUETES DE VOZ SOBRE UNA RED IP.

IAX2 utiliza un único puerto UDP, generalmente el 4569, para comunicaciones entre puntos finales (terminales VoIP) para señalización y datos. El tráfico de voz es transmitido in-band, lo que hace a IAX2 un protocolo casi transparente a los cortafuegos (Firewall) y realmente eficaz para trabajar dentro de redes internas. En esto se diferencia de SIP, que utiliza una cadena RTP out-of-band para entregar la información. (Anaya, 2018).

PBX: Las PBX tradicionales tendrían sus propios teléfonos propietarios, por lo que no existiría una forma de utilizar estos teléfonos con un sistema diferente. Esto significa que ya sea que tengamos un system-lock-in (estamos limitados al mismo sistema ya que un cambio de sistema significa también cambiar teléfonos, lo que lo hace prohibitivo y de un alto costo) o

un vendor-lock-in (estamos limitados al mismo fabricante debido a que los teléfonos solo se pueden utilizar con sistemas de ese fabricante, algunas veces sólo con un rango particular de sistemas).

El tiempo y la tecnología, sin embargo, han cambiado el panorama de consumo de telefonía, siendo la PBX IP basada en estándares abiertos la que abanderara este terreno. El punto de "IP" en esta era es que las llamadas telefónicas son entregadas utilizando el Protocolo de Internet como la tecnología de transporte. (3CX, 2018)

SIP: por sus siglas en inglés "Session Initiation Protocol" (Protocolo de inicio de sesión), es un protocolo de señalización de telefonía IP o videoconferencia, utilizado para establecer, modificar y terminar llamadas VoIP o una videoconferencia. SIP fue desarrollado por el IETF y publicado como RFC 3261.

Hoy en día es el estándar más usado en VoIP, prácticamente todos los fabricantes de teléfonos IP y conmutadores IP basan su tecnología en el protocolo SIP.

SIP describe la comunicación necesaria para establecer una llamada telefónica. SIP ha tomado el mundo VoIP por sorpresa. El protocolo es parecido al protocolo HTTP, es basado en texto, muy abierto y flexible. Consecuentemente ha reemplazado el estándar H323. (Teleradio, 2018)

VOIP: proviene del inglés Voice Over Internet Protocol, que significa "voz sobre un protocolo de internet". Básicamente VoIP es un método por el cual tomando señales de audio analógicas del tipo de las que se escuchan cuando uno habla por teléfono se las transforma en datos digitales que pueden ser transmitidos a través de internet hacia una dirección IP determinada. El VoIP permite la unión de dos mundos históricamente separados, el de la transmisión de voz y el de la transmisión de datos. Entonces, el VoIP no es un servicio sino una tecnología. VoIP puede transformar una conexión standard a internet en una plataforma para

realizar llamadas gratuitas por internet. Usando algunos de los software gratuitos para llamadas VoIP que están disponibles en internet estamos salteándonos a las compañías tradicionales de telefonía, y por consiguiente, sus tarifas.

En el pasado, las conversaciones mediante VoIP solían ser de baja calidad, esto se vio superado por la tecnología actual y la proliferación de conexiones de banda ancha, hasta tal punto llego la expansión de la telefonía ip que existe la posibilidad de que usted sin saberlo ya haya utilizado un servicio VoIP, por ejemplo, las operadoras de telefonía convencional, utilizan los servicios del VoIP para transmitir llamadas de larga distancia y de esta forma reducir costos.

Se sabe que va a llevar algún tiempo, pero es seguro que en un futuro cercano desaparecerán por completo las líneas de teléfono convencionales que utilizamos en nuestra vida cotidiana, el avance tecnológico indica que estas serán muy probablemente reemplazadas por la telefonía IP. (VOIP, 2018)

VPN: son las siglas de Virtual Private Network, o red privada virtual que, a diferencia de otras palabras informáticas más crípticas como DNS o HTTP, sí nos dan pistas bastante precisas sobre en qué consisten.

La palabra clave aquí es virtual, pues es esta propiedad la que genera la necesidad de la VPN en sí, así como la que permite a las conexiones VPN ofrecerte los múltiples usos que veremos más adelante.

Para conectarse a Internet, tu móvil, PC, televisión y demás dispositivos generalmente se comunican con el router o módem que conecta tu casa con tu proveedor de Internet, ya sea mediante cable o inalámbricamente. Los componentes son distintos si estás usando la conexión de datos de tu móvil (que incluye su propio módem y habla con la antena de telefonía) pero la esencia es la misma: tu dispositivo se conecta a otro, que le conecta a Internet.

Lo más normal es que no tengas uno, sino varios dispositivos conectados al mismo router: móviles, ordenadores, consolas... En este caso cada uno tendrá asignada una dirección IP local, que no es visible desde Internet. Esto es una red local, un conjunto de dispositivos conectados de tal modo que puedan compartir archivos e impresoras sin necesidad de pasar por Internet.

Una conexión VPN lo que te permite es crear una red local sin necesidad que sus integrantes estén físicamente conectados entre sí, sino a través de Internet. Es el componente "virtual" del que hablábamos antes. Obtienes las ventajas de la red local (y alguna extra), con una mayor flexibilidad, pues la conexión es a través de Internet y puede por ejemplo ser de una punta del mundo a la otra. (Ramírez, 2018)

WAN: La llamada Red de Area Amplia, o WAN (Wide Area Network) como también se la conoce es básicamente una o más redes LAN interconectadas entre sí para poder abarcar mucho más territorio, a veces incluso, hasta continentes.

Las redes WAN son mayormente utilizadas por grandes compañías para su propio uso, mientras que otras WAN son utilizadas por ISP para ofrecerle el servicio de Internet a su clientela. Las computadoras conectadas a través de una Red de Area Amplia o WAN generalmente se encuentran conectados a través de redes públicas tales como el sistema telefónico, sin embargo también pueden valerse de satélites y otros mecanismos. (Informática, 2018).

CAPITULO III

METODOLOGIA DE LA INVESTIGACIÓN

3.1 Metodología de la investigación

En la presente investigación se usará la metodología PTES (Penetration Testing Execution Standart) consta de siete secciones principales. Estos cubren todo lo relacionado con una prueba de penetración:

a) Herramientas requeridas

Son esos programas, aplicaciones o simplemente instrucciones usadas para efectuar otras tareas de modo más sencillo. En un sentido amplio del término, podemos decir que una herramienta es cualquier programa o instrucción que facilita una tarea, pero también podríamos hablar del hardware o accesorios como herramientas. (seguridad, 2017)

b) Recolección de información

Recopilación de información de inteligencia competitiva publicada en motores de búsqueda que nos dará una idea del objetivo que estamos estudiando y de las personas que trabajan dentro de la empresa.

Normalmente en esta fase debemos obtener toda la información posible para diseñarnos o imaginarnos como está distribuida la red a penetrar.

Las guías de CEH nos enumeran siete Etapas de Information Gathering
- Footprinting

- ❖ Gathering information
- ❖ Locating the network range
- ❖ Identifying active machines
- ❖ Finding open ports and applications
- ❖ Detecting operating systems
- ❖ Fingerprinting services
- ❖ Mapping the network

Footprinting

Es definido como el proceso de crear un modelo o mapa de una organización de redes y sistemas. Consiste en la búsqueda de toda la información pública, bien porque haya sido publicada a propósito o bien porque haya sido publicada por desconocimiento. en este proceso buscaremos todas las huellas posibles, como direcciones IP, servidores internos, cuentas de correo de los usuarios, nombres de máquinas, información del registrador del dominio, tipos de servidores, ficheros con cuentas y/o credenciales de usuarios, impresoras, cámaras IP, metadatos, etc.

Fingerprinting

Es un proceso o técnica que consiste en analizar y determinar las huellas que deja un S.O en sus conexiones de red.

Los programas que se utilizan para realizar Fingerprinting se basan en dos filosofías, escáner pasivo o activo:

Activo: Cuando se envía paquetes esperando respuesta del objetivo y es comparada con su base de datos, las técnicas que suelen ser usadas son: inundación de paquetes SYN, envío flags TCP incorrectos, envío de paquetes FIN... los cuales permiten ser detectados fácilmente.

Pasivo: Cuando se esnifea tráfico para identificar las máquinas que se intercomunican en la red, comparando sus tiempos de respuesta sin actuar en la red. La detección de esta técnica se torna difícil, pero tiene sus inconvenientes: hay que esperar un gran lapso de tiempo para la captura de paquetes. (Atoio, 2018)

c) Análisis de vulnerabilidades

Como su propio nombre indica entramos en materia. De forma activa y ya 'tocando' el objetivo, se identifican puertos y servicios existentes en busca, de forma manual y automática vulnerabilidades existentes.

En este apartado básicamente se define el ámbito y alcance del test de intrusión. Se llega a un acuerdo con el cliente acotando la profundidad de las pruebas a realizar, permisividad de ataques (ataques DOS, fuerza bruta...), enfoque del test (caja negra, gris o blanca) presentación de evidencias (goals), etc.

Se trata de un análisis cuyo objetivo es identificar e informar de los errores o fallas en los dispositivos y en los procesos tecnológicos.

Es importante destacar que este tipo de análisis no incluye la explotación de las vulnerabilidades identificadas, sino que solo identifica esas vulnerabilidades y las presenta, pero no son explotadas o aprovechadas.

Habitualmente, este tipo de análisis está relacionado con la identificación de puertos abiertos, servicios disponibles y

vulnerabilidades conocidas en los sistemas de información, pudiendo las mismas incurrir en los famosos falsos positivos(muchas veces debido solo al uso de herramientas automatizadas para detección de vulnerabilidades).

No obstante, este tipo de análisis permite identificar puntos débiles de la red y de nuestros sistemas, orientando al usuario de aquello que provoca que el sistema sea vulnerable y permitiendo, por tanto, tomar medidas correctivas para solventar esas vulnerabilidades. (SegInfoSys, 2018)

d) Explotación

Con la información proporcionada por las dos fases anteriores, se definen líneas de negocios existentes, importancia de los activos IT (accesibles) visibles en nuestro estudio para definir vectores de ataques posteriores.

Un test de penetración consiste en pruebas ofensivas contra los mecanismos de defensa existentes en el entorno que se está analizando. Estas pruebas comprenden desde el análisis de dispositivos físicos y digitales, hasta el análisis del factor humano utilizando Ingeniería Social.

El objetivo de estas pruebas es verificar bajo situaciones extremas cuál es el comportamiento de los mecanismos de defensa, específicamente, se busca detectar vulnerabilidades en los mismos. Además, se identifican aquellas faltas de controles y las brechas que pueden existir entre la información crítica y los controles existentes.

Existen muchos casos donde las organizaciones sufren incidentes que podrían haberse evitado si los mecanismos de protección hubieran sido reforzados en su momento. Los incidentes comprenden sucesos tales como fuga de información, accesos no autorizados, pérdida de datos, entre muchos otros. El análisis de los mecanismos de protección debe ser una tarea proactiva permitiendo al pentester (persona que lleva adelante la auditoría) encontrar las vulnerabilidades dentro de los

mismos y brindar una solución antes de que un ciberdelincuente aproveche esta debilidad. (Catoira, 2012)

e) **Post-explotación**

Esta fase se centra en la recopilación de evidencias y en cómo valorar el impacto real de la intrusión y hasta donde podemos llegar desde el sistema comprometido. Se contempla borrado de huellas y hacer persistente el ataque (puertas traseras, conexión inversa o rootkits)


f) **Informes**



Explica qué deben contener los reportes (ejecutivo y técnico) que entreguemos como conclusión de nuestro estudio



Esta metodología maneja niveles de riesgo dirigidos a un lenguaje para el negocio y maneja una descripción cualitativa, lo que permite la fácil comunicación con el cliente. Las razones para las que se solicitó el test deben ser los primeros aspectos relevantes del informe final. Seguimiento de los posibles riesgos y su valoración. Las métricas utilizadas y las contra medidas propuestas para los riesgos analizados.

3.2 Herramientas

A continuación, se detallan las herramientas software para el proceso de Pentesting:

HERRAMIENTA	DESCRIPCION
 Cain y Abel	Cain & Abel es una herramienta de recuperación de contraseña para sistemas operativos de Microsoft. Permite la recuperación fácil de varios tipos de contraseñas mediante el rastreo de la red,

	<p>descifrando contraseñas cifradas mediante ataques de Diccionario, Brute-Force y Cryptanalysis, grabando conversaciones VoIP, descodificando contraseñas codificadas, recuperando claves de red inalámbrica, revelando cuadros de contraseñas, descubriendo contraseñas almacenadas en caché y analizando el enrutamiento protocolos El programa no explota ninguna vulnerabilidad de software o error que no pueda solucionarse con poco esfuerzo. Cubre algunos aspectos de seguridad / debilidad presentes en los estándares del protocolo, los métodos de autenticación y los mecanismos de almacenamiento en caché; su propósito principal es la recuperación simplificada de contraseñas y credenciales de varias fuentes, sin embargo, también incluye algunas utilidades "no estándar" para los usuarios de Microsoft Windows.</p>
 FreePBX	<p>Es un panel de configuración web open source para Asterisk, que fue creado hace años para poder realizar de una forma gráfica y sencilla la configuración de entradas, salidas, dialplan y funciones específicas de Asterisk de forma gráfica y que no requiriera de unos conocimientos elevados de programación de dialplan de Asterisk..</p>
 Nmap	<p>Es una utilidad de software libre para explorar, administrar y auditar la seguridad de redes de ordenadores. Detecta hosts online, sus puertos abiertos, servicios y aplicaciones</p>

	<p>corriendo en ellos, su sistema operativo, que firewalls/filtros corren en una red y de que tipo son. Es excelente para hacer trabajos de auditoria de res y fue diseñado para llevar acabo escaneos rápidos en una gran cantidad de redes, pero es igualmente usable en hosts individuales. Es reconocido como el scanner de puertos mas poderoso.</p>
 sipvicious	<p>es una utilidad que podemos usar para probar si la configuración SIP de nuestro servidor Asterisk es segura. Se compone de cuatro programas, escritos en lenguaje Python: ... svcrack: Intenta obtener la contraseña de una extensión SIP en un servidor PBX. svreport: Genera reportes de diferente tipo</p>
 WireShark	<p>La herramienta intercepta el tráfico y lo convierte en un formato legible para las personas. Esto hace que sea más fácil identificar qué tráfico está cruzando la red, con qué frecuencia y la latencia que hay entre ciertos saltos. Si bien Wireshark admite más de 2.000 protocolos de red, muchos de ellos inusuales o antiguos, los profesionales encuentran una gran utilidad en el análisis de identidades IP. La mayoría de los paquetes son TCP, UDP e ICMP.</p>

CAPÍTULO IV

DESARROLLO E IMPLEMENTACION

4.1. Desarrollo e Implementación

DOCUMENTACION PENTESTING SERVIDOR VOIP

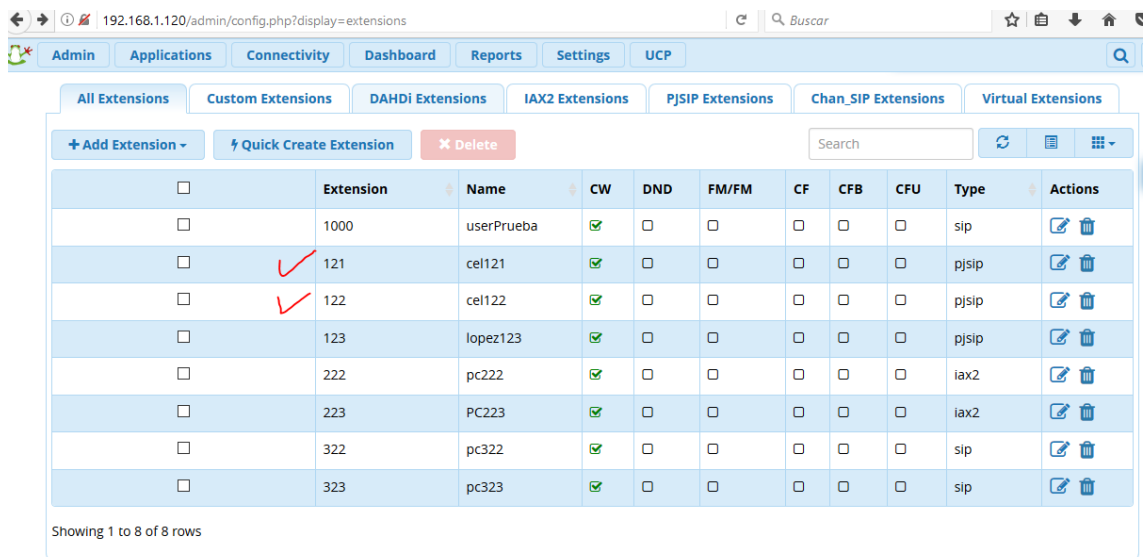
ATAQUE: MAN IN THE MIDDLE – ARP SPOOFING (INTERCEPCION DE LLAMADAS)

Se tiene la siguiente estructura de red



Se procede con el acceso al servidor abriendo el navegador e ingresando la dirección IP: 192.168.1.120. Si es q nos saliera el mensaje en rojo al ingresar al server mediante el navegador: **cannot connect to Asterisk**, entonces lo q tendríamos q hacer en el prompt del server: **fwconsole restart**

Se procede a visualizar las extensiones en el servidor voip

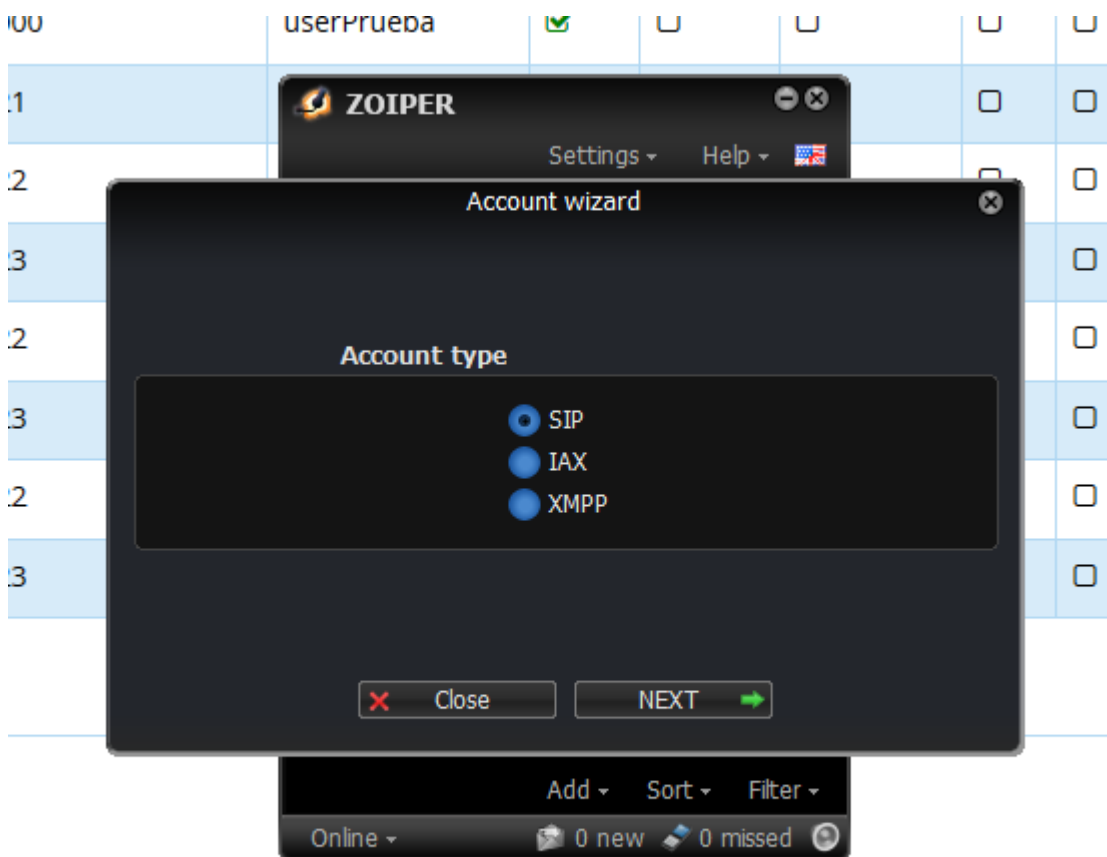


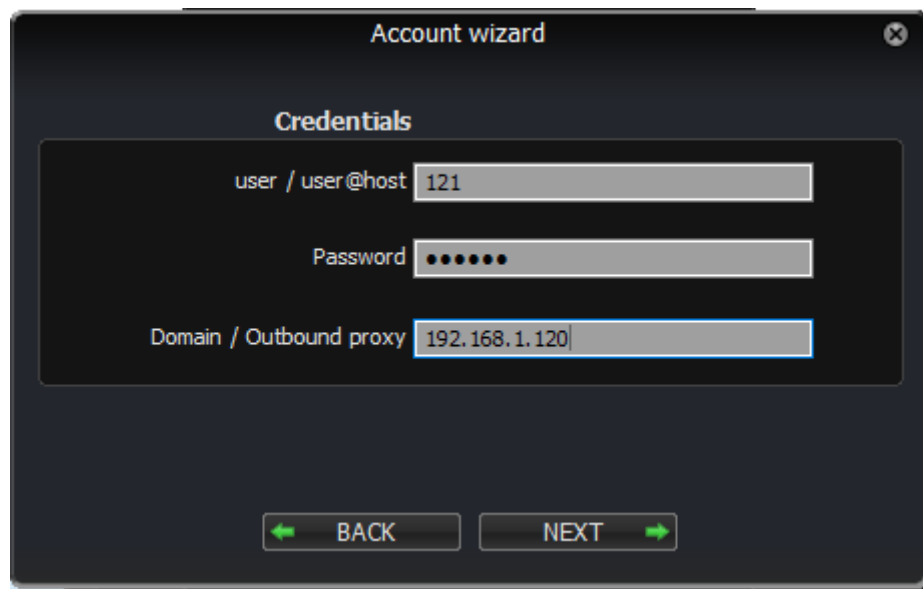
The screenshot shows the Asterisk Extensions Management web interface. The browser address bar displays '192.168.1.120/admin/config.php?display=extensions'. The interface includes a navigation menu with tabs: Admin, Applications, Connectivity, Dashboard, Reports, Settings, and UCP. Below the navigation menu, there are tabs for extension types: All Extensions, Custom Extensions, DAHDi Extensions, IAX2 Extensions, PJSIP Extensions, Chan_SIP Extensions, and Virtual Extensions. A toolbar contains buttons for '+ Add Extension', 'Quick Create Extension', and 'Delete', along with a search bar and icons for refresh, list, and grid views. The main content area is a table with the following columns: Extension, Name, CW, DND, FM/FM, CF, CFB, CFU, Type, and Actions. The table lists 8 extensions, with extensions 121 and 122 marked with red checkmarks. The footer indicates 'Showing 1 to 8 of 8 rows'.

	Extension	Name	CW	DND	FM/FM	CF	CFB	CFU	Type	Actions
<input type="checkbox"/>	1000	userPrueba	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	sip	
<input type="checkbox"/>	121	cel121	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	pjsip	
<input type="checkbox"/>	122	cel122	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	pjsip	
<input type="checkbox"/>	123	lopez123	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	pjsip	
<input type="checkbox"/>	222	pc222	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	iax2	
<input type="checkbox"/>	223	PC223	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	iax2	
<input type="checkbox"/>	322	pc322	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	sip	
<input type="checkbox"/>	323	pc323	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	sip	

Showing 1 to 8 of 8 rows

En la maquina 192.168.1.21, crearemos la extensión 121



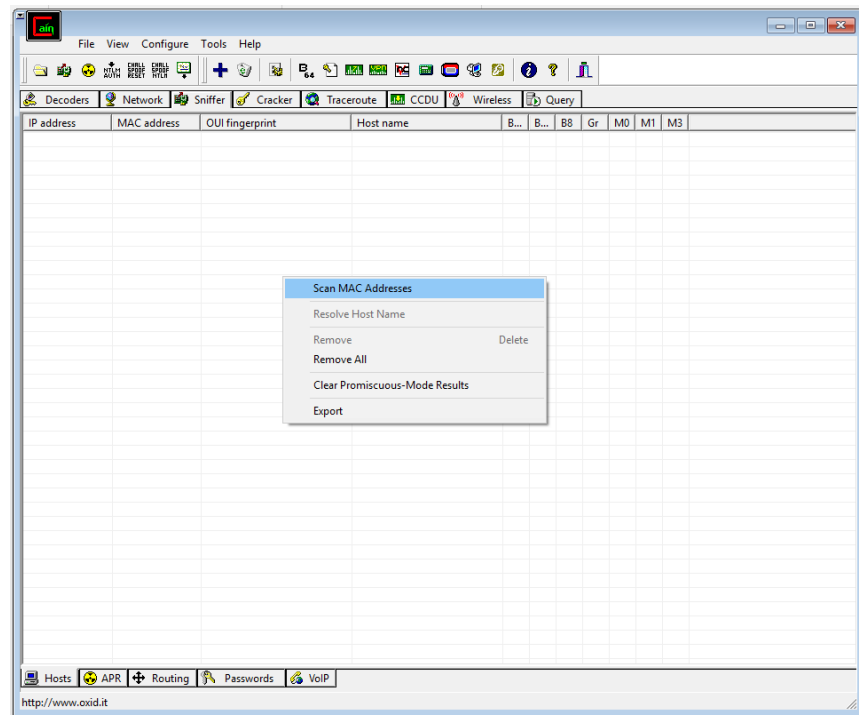


El mismo procedimiento se hará en la maquina 192.168.1.62 pero con la extensión 122

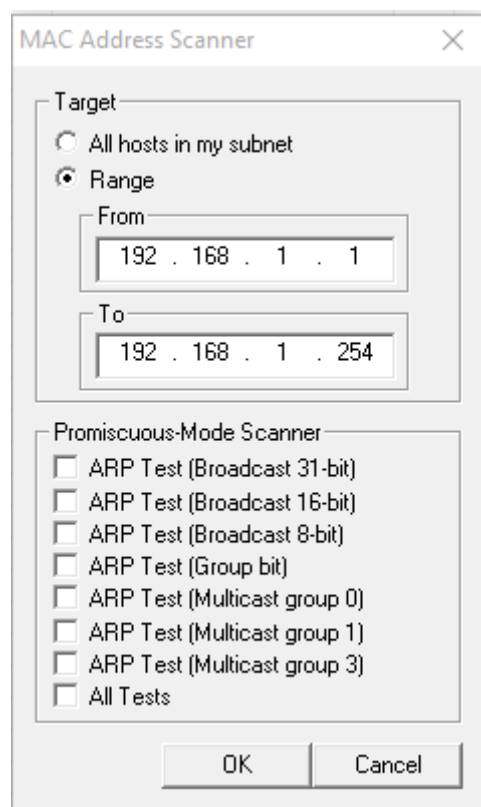
Hacer la configuración de audio y micrófono en los clientes

Ahora en la maquina atacante (192.168.1.14) haremos los siguientes pasos

- Primero instalar el wireshark y cain y Abel
- Desactivar el cortafuego del atacante (192.168.1.14)
- Procedemos con el proceso del envenamiento ARP
- Abrimos cain y Abel y clic en START SNIFFER
- En la ficha sniifer clic derecho y SCAN ADDRES



Especificamos el rango



A continuación nos muestra lo siguiente:

Handwritten annotations in blue:

- Victima** (Victim) with an arrow pointing to the destination IP 192.168.1.120.
- cliente 2** (Client 2) with an arrow pointing to the source IP 192.168.1.121.
- Server** with an arrow pointing to the source IP 192.168.1.120.

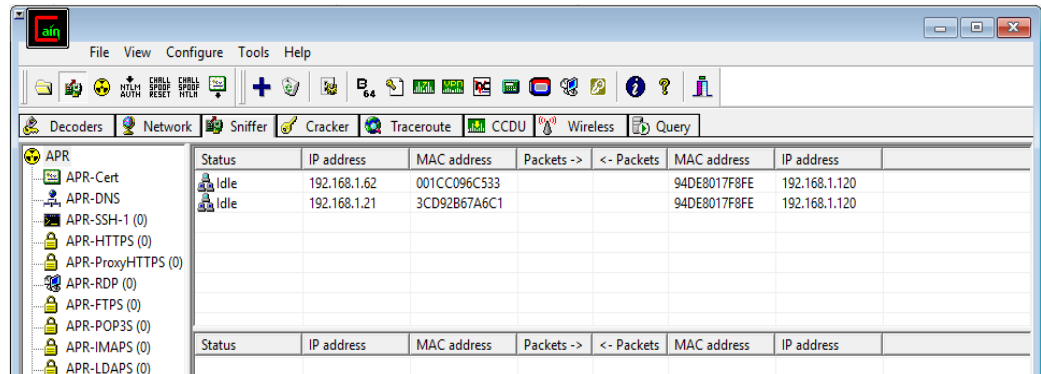
The packet list shows a ping request from 192.168.1.121 to 192.168.1.120.

IP address	MAC address	OUI fingerprint	Host name	B...	B...	B8	Gr	M0	M1
192.168.1.9	2C4138B4C94F	Hewlett-Packard Company							
192.168.1.1	BC968050F7F2	Shenzhen Gongjin Electroni...							
192.168.1.18	001CC096C572	Intel Corporate							
192.168.1.21	3CD92B67A6C1	Hewlett-Packard Company							
192.168.1.23	3CD92B67A68C	Hewlett-Packard Company							
192.168.1.30	2C4138AF9B79	Hewlett-Packard Company							
192.168.1.34	001CC096C54D	Intel Corporate							
192.168.1.24	2CAE284BB37								
192.168.1.26	1CCB996C2C1F								
192.168.1.39	80C16EE3B0E2	Hewlett Packard							
192.168.1.40	E839355C747E	Hewlett Packard							
192.168.1.41	001CC096C570	Intel Corporate							
192.168.1.38	B4527E7BEBBB	Sony Mobile Communicatio...							
192.168.1.62	001CC096C533	Intel Corporate							
192.168.1.12	78C3E92591A0								
192.168.1.11	AC18269D2624	SEIKO EPSON CORPORATION							
192.168.1.120	94DE8017F8FE	GIGA-BYTE TECHNOLOGY ...							

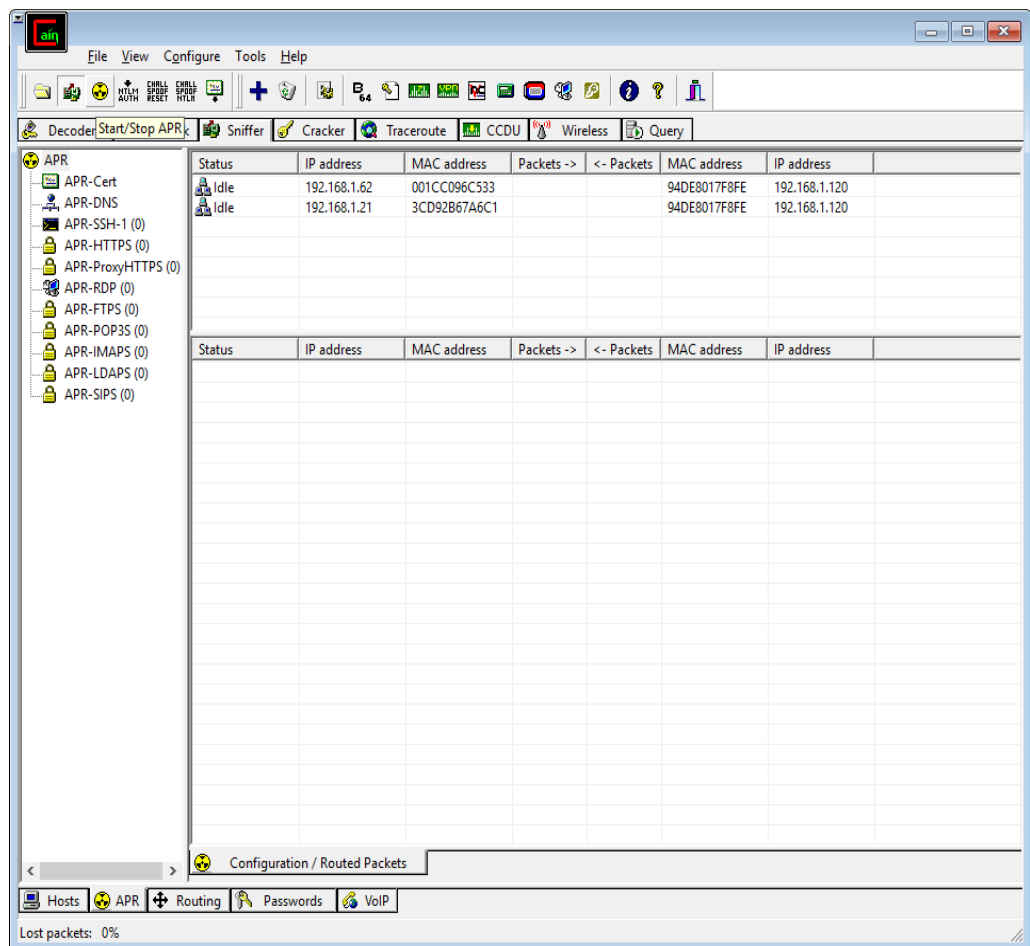
Luego irnos a la ficha ARP y clic en el botón ADD TO LIST

The screenshot displays the Wireshark network protocol analyzer interface. The left-hand pane (Protocol Hierarchy) shows a tree structure with 'APR' expanded, listing various protocols such as APR-Cert, APR-DNS, APR-SSH-1 (0), APR-HTTPS (0), APR-ProxyHTTPS (0), APR-RDP (0), APR-FTPS (0), APR-POP3S (0), APR-IMAPS (0), APR-LDAPS (0), and APR-SIPS (0). The main display area (Packet List and Packet Details) is currently empty, showing two tables with columns: Status, IP address, MAC address, Packets ->, <- Packets, MAC address, and IP address. The bottom status bar indicates 'Lost packets: 0%'. The top menu bar includes File, View, Configure, Tools, and Help. The top toolbar contains icons for various functions like opening files, saving, and network-related actions. The bottom toolbar shows tabs for Hosts, APR, Routing, Passwords, and VoIP.

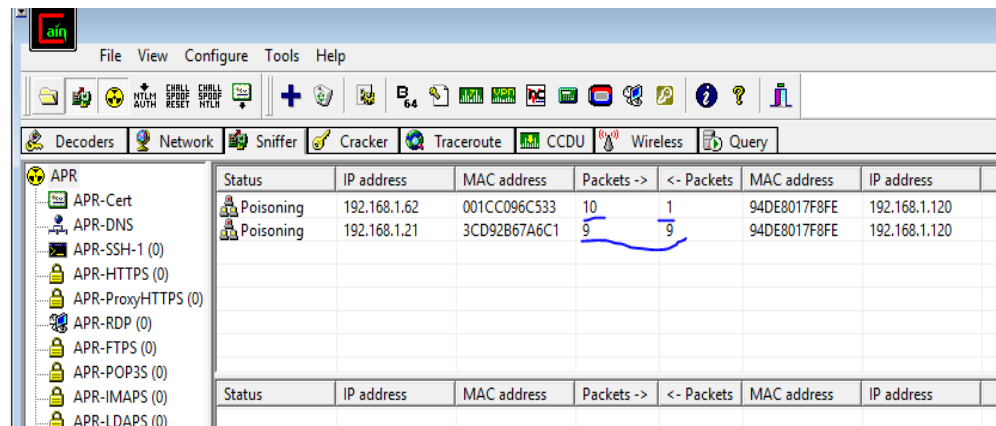
Escoger todas las pcs q involucran dicha ruta



Y Clic en el botón START POISONING

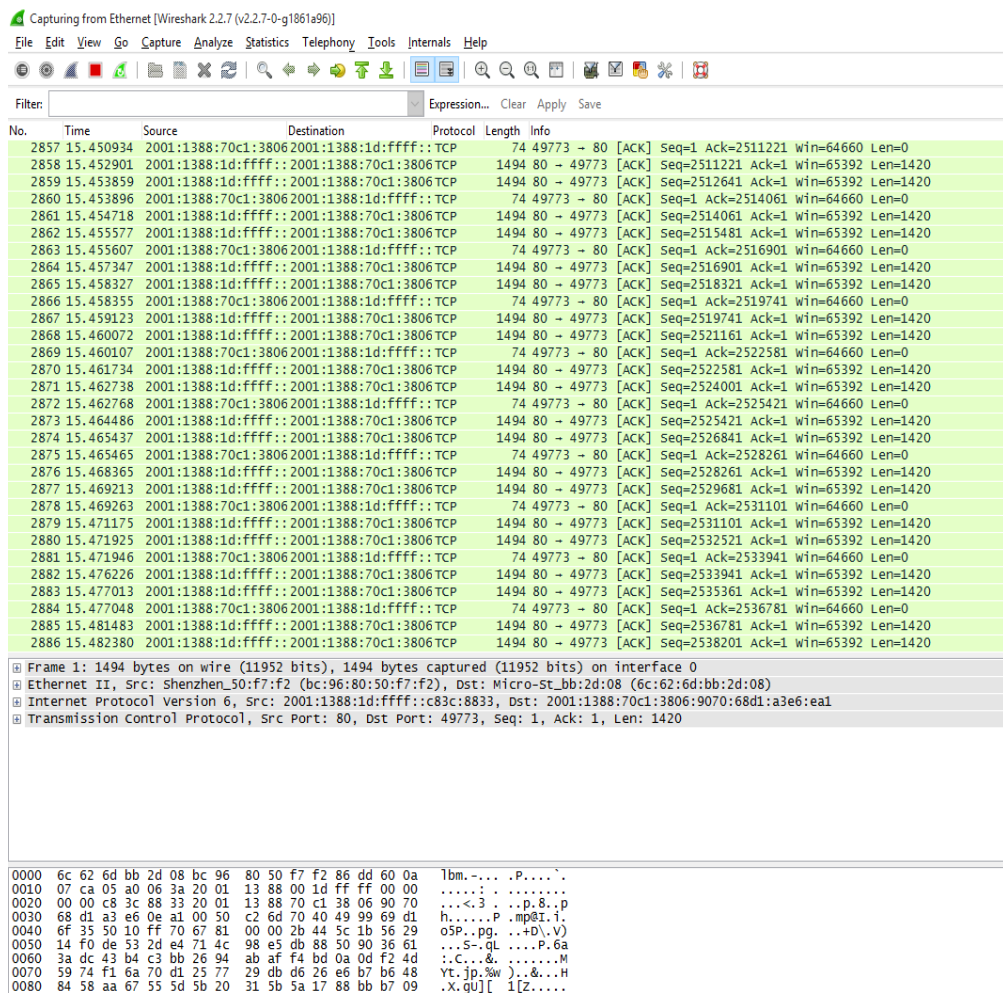


Antes debemos esperar q haya actividad en la red mejor dicho que se incremente la cantidad de paquetes:



Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address
Poisoning	192.168.1.62	001CC096C533	10	1	94DE8017F8FE	192.168.1.120
Poisoning	192.168.1.21	3CD92B67A6C1	9	9	94DE8017F8FE	192.168.1.120

Luego ejecutar el sniffer (wireshark)



No.	Time	Source	Destination	Protocol	Length	Info
2857	15.450934	2001:1388:70c1:3806	2001:1388:1d:ffff::	TCP	74	49773 → 80 [ACK] Seq=1 Ack=2511221 Win=64660 Len=0
2858	15.452901	2001:1388:1d:ffff::	2001:1388:70c1:3806	TCP	1494	80 → 49773 [ACK] Seq=2511221 Ack=1 Win=65392 Len=1420
2859	15.453859	2001:1388:1d:ffff::	2001:1388:70c1:3806	TCP	1494	80 → 49773 [ACK] Seq=2512641 Ack=1 Win=65392 Len=1420
2860	15.453896	2001:1388:70c1:3806	2001:1388:1d:ffff::	TCP	74	49773 → 80 [ACK] Seq=1 Ack=2514061 Win=64660 Len=0
2861	15.454718	2001:1388:1d:ffff::	2001:1388:70c1:3806	TCP	1494	80 → 49773 [ACK] Seq=2514061 Ack=1 Win=65392 Len=1420
2862	15.455577	2001:1388:1d:ffff::	2001:1388:70c1:3806	TCP	1494	80 → 49773 [ACK] Seq=2515481 Ack=1 Win=65392 Len=1420
2863	15.455607	2001:1388:70c1:3806	2001:1388:1d:ffff::	TCP	74	49773 → 80 [ACK] Seq=1 Ack=2516901 Win=64660 Len=0
2864	15.457347	2001:1388:1d:ffff::	2001:1388:70c1:3806	TCP	1494	80 → 49773 [ACK] Seq=2516901 Ack=1 Win=65392 Len=1420
2865	15.458327	2001:1388:1d:ffff::	2001:1388:70c1:3806	TCP	1494	80 → 49773 [ACK] Seq=2518321 Ack=1 Win=65392 Len=1420
2866	15.458355	2001:1388:70c1:3806	2001:1388:1d:ffff::	TCP	74	49773 → 80 [ACK] Seq=1 Ack=2519741 Win=64660 Len=0
2867	15.459123	2001:1388:1d:ffff::	2001:1388:70c1:3806	TCP	1494	80 → 49773 [ACK] Seq=2519741 Ack=1 Win=65392 Len=1420
2868	15.460072	2001:1388:1d:ffff::	2001:1388:70c1:3806	TCP	1494	80 → 49773 [ACK] Seq=2521161 Ack=1 Win=65392 Len=1420
2869	15.460107	2001:1388:70c1:3806	2001:1388:1d:ffff::	TCP	74	49773 → 80 [ACK] Seq=1 Ack=2522581 Win=64660 Len=0
2870	15.461734	2001:1388:1d:ffff::	2001:1388:70c1:3806	TCP	1494	80 → 49773 [ACK] Seq=2522581 Ack=1 Win=65392 Len=1420
2871	15.462738	2001:1388:1d:ffff::	2001:1388:70c1:3806	TCP	1494	80 → 49773 [ACK] Seq=2524001 Ack=1 Win=65392 Len=1420
2872	15.462768	2001:1388:70c1:3806	2001:1388:1d:ffff::	TCP	74	49773 → 80 [ACK] Seq=1 Ack=2525421 Win=64660 Len=0
2873	15.464486	2001:1388:1d:ffff::	2001:1388:70c1:3806	TCP	1494	80 → 49773 [ACK] Seq=2525421 Ack=1 Win=65392 Len=1420
2874	15.465437	2001:1388:1d:ffff::	2001:1388:70c1:3806	TCP	1494	80 → 49773 [ACK] Seq=2526841 Ack=1 Win=65392 Len=1420
2875	15.465465	2001:1388:70c1:3806	2001:1388:1d:ffff::	TCP	74	49773 → 80 [ACK] Seq=1 Ack=2528261 Win=64660 Len=0
2876	15.468365	2001:1388:1d:ffff::	2001:1388:70c1:3806	TCP	1494	80 → 49773 [ACK] Seq=2528261 Ack=1 Win=65392 Len=1420
2877	15.469213	2001:1388:1d:ffff::	2001:1388:70c1:3806	TCP	1494	80 → 49773 [ACK] Seq=2529681 Ack=1 Win=65392 Len=1420
2878	15.469263	2001:1388:70c1:3806	2001:1388:1d:ffff::	TCP	74	49773 → 80 [ACK] Seq=1 Ack=2531101 Win=64660 Len=0
2879	15.471175	2001:1388:1d:ffff::	2001:1388:70c1:3806	TCP	1494	80 → 49773 [ACK] Seq=2531101 Ack=1 Win=65392 Len=1420
2880	15.471925	2001:1388:1d:ffff::	2001:1388:70c1:3806	TCP	1494	80 → 49773 [ACK] Seq=2532521 Ack=1 Win=65392 Len=1420
2881	15.471946	2001:1388:70c1:3806	2001:1388:1d:ffff::	TCP	74	49773 → 80 [ACK] Seq=1 Ack=2533941 Win=64660 Len=0
2882	15.476226	2001:1388:1d:ffff::	2001:1388:70c1:3806	TCP	1494	80 → 49773 [ACK] Seq=2533941 Ack=1 Win=65392 Len=1420
2883	15.477013	2001:1388:1d:ffff::	2001:1388:70c1:3806	TCP	1494	80 → 49773 [ACK] Seq=2535361 Ack=1 Win=65392 Len=1420
2884	15.477048	2001:1388:70c1:3806	2001:1388:1d:ffff::	TCP	74	49773 → 80 [ACK] Seq=1 Ack=2536781 Win=64660 Len=0
2885	15.481483	2001:1388:1d:ffff::	2001:1388:70c1:3806	TCP	1494	80 → 49773 [ACK] Seq=2536781 Ack=1 Win=65392 Len=1420
2886	15.482380	2001:1388:1d:ffff::	2001:1388:70c1:3806	TCP	1494	80 → 49773 [ACK] Seq=2538201 Ack=1 Win=65392 Len=1420

[1] Frame 1: 1494 bytes on wire (11952 bits), 1494 bytes captured (11952 bits) on interface 0
 [2] Ethernet II, Src: Shenzhen_50:f7:f2 (bc:96:80:50:f7:f2), Dst: Micro-st_bb:2d:08 (6c:62:6d:bb:2d:08)
 [3] Internet Protocol Version 6, Src: 2001:1388:1d:ffff::c83c:8833, Dst: 2001:1388:70c1:3806:9070:68d1:a3e6:ea1
 [4] Transmission Control Protocol, Src Port: 80, Dst Port: 49773, Seq: 1, Ack: 1, Len: 1420

```

0000  6c 62 6d bb 2d 08 bc 96 80 50 f7 f2 86 dd 60 0a  1bm....P....
0010  07 ca 05 a0 06 3a 20 01 13 88 00 1d ff ff 00 00  .....
0020  00 00 c8 3c 88 33 20 01 13 88 70 c1 38 06 90 70  ...<3...pB..
0030  68 d1 a3 e6 0e a1 00 50 c2 6d 70 40 49 99 69 d1  h.....P.mpe1.
0040  6f 35 50 10 ff 70 67 81 00 00 2b 44 5c 1b 56 29  o5P.pg...+D.V
0050  14 f0 de 53 2d e4 71 4c 98 e5 db 88 50 90 36 61  ...S..qL...P.6a
0060  3a dc 43 b4 c3 bb 26 94 ab af f4 bd 0a 0d f2 4d  ..C...&.....M
0070  59 74 f1 6a 70 d1 25 77 29 db d6 26 e6 b7 b6 48  Yt.jp.%w)...&H
0080  84 58 aa 67 55 5d 5b 20 31 5b 5a 17 88 bb b7 09  .x.gu][1Z....
  
```

Y realizar las llamadas

Luego que en los clientes hayan colgados la llamada, en el atacante detener el snifer y cómo podemos ver se hizo la captura de los paquetes RTP

*Ethernet [Wireshark 2.2.7 (v2.2.7-0-g1861a96)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

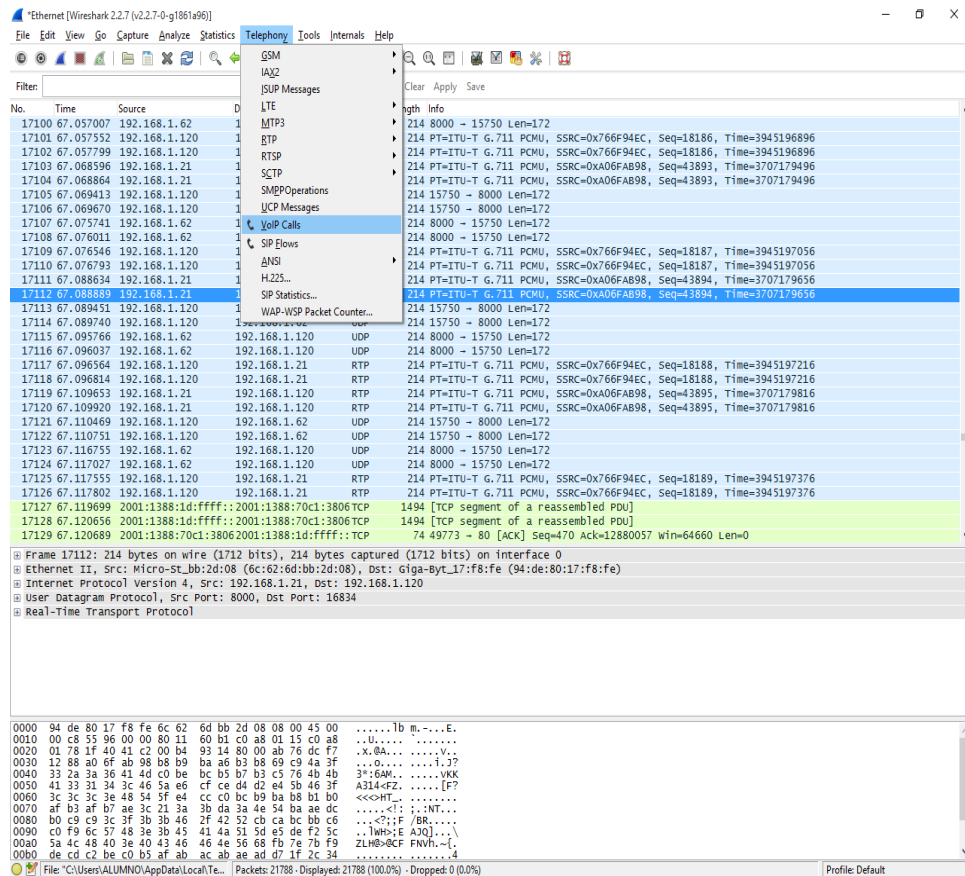
No.	Time	Source	Destination	Protocol	Length	Info
17100	67.057007	192.168.1.62	192.168.1.120	UDP	214	8000 → 15750 Len=172
17101	67.057552	192.168.1.120	192.168.1.21	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x766F94EC, Seq=18186, T
17102	67.057799	192.168.1.120	192.168.1.21	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x766F94EC, Seq=18186, T
17103	67.068596	192.168.1.21	192.168.1.120	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0xA06FAB98, Seq=43893, T
17104	67.068864	192.168.1.21	192.168.1.120	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0xA06FAB98, Seq=43893, T
17105	67.069413	192.168.1.120	192.168.1.62	UDP	214	15750 → 8000 Len=172
17106	67.069670	192.168.1.120	192.168.1.62	UDP	214	15750 → 8000 Len=172
17107	67.075741	192.168.1.62	192.168.1.120	UDP	214	8000 → 15750 Len=172
17108	67.076011	192.168.1.62	192.168.1.120	UDP	214	8000 → 15750 Len=172
17109	67.076546	192.168.1.120	192.168.1.21	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x766F94EC, Seq=18187, T
17110	67.076793	192.168.1.120	192.168.1.21	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x766F94EC, Seq=18187, T
17111	67.088634	192.168.1.21	192.168.1.120	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0xA06FAB98, Seq=43894, T
17112	67.088889	192.168.1.21	192.168.1.120	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0xA06FAB98, Seq=43894, T
17113	67.089451	192.168.1.120	192.168.1.62	UDP	214	15750 → 8000 Len=172
17114	67.089740	192.168.1.120	192.168.1.62	UDP	214	15750 → 8000 Len=172
17115	67.095766	192.168.1.62	192.168.1.120	UDP	214	8000 → 15750 Len=172
17116	67.096037	192.168.1.62	192.168.1.120	UDP	214	8000 → 15750 Len=172
17117	67.096564	192.168.1.120	192.168.1.21	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x766F94EC, Seq=18188, T
17118	67.096814	192.168.1.120	192.168.1.21	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x766F94EC, Seq=18188, T
17119	67.109653	192.168.1.21	192.168.1.120	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0xA06FAB98, Seq=43895, T
17120	67.109920	192.168.1.21	192.168.1.120	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0xA06FAB98, Seq=43895, T
17121	67.110469	192.168.1.120	192.168.1.62	UDP	214	15750 → 8000 Len=172
17122	67.110751	192.168.1.120	192.168.1.62	UDP	214	15750 → 8000 Len=172
17123	67.116755	192.168.1.62	192.168.1.120	UDP	214	8000 → 15750 Len=172
17124	67.117027	192.168.1.62	192.168.1.120	UDP	214	8000 → 15750 Len=172
17125	67.117555	192.168.1.120	192.168.1.21	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x766F94EC, Seq=18189, T
17126	67.117802	192.168.1.120	192.168.1.21	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x766F94EC, Seq=18189, T
17127	67.119699	2001:1388:1d:ffff::2001:1388:70c1:3806	TCP	1494	[TCP segment of a reassembled PDU]	
17128	67.120656	2001:1388:1d:ffff::2001:1388:70c1:3806	TCP	1494	[TCP segment of a reassembled PDU]	
17129	67.120689	2001:1388:70c1:3806	2001:1388:1d:ffff::TCP	74	49773 → 80 [ACK] Seq=470 Ack=12880057 win=64660 Le	

Frame 17112: 214 bytes on wire (1712 bits), 214 bytes captured (1712 bits) on interface 0

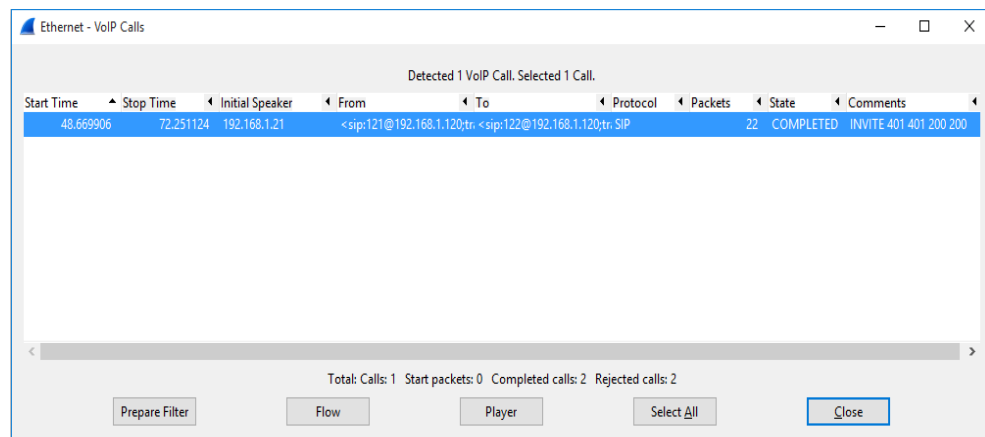
Ethernet II, Src: Micro-St_bb2d:08 (6c:62:6d:bb:2d:08), Dst: Giga-Byt_17:f8:fe (94:de:80:17:f8:fe)

Internet Protocol Version 4, Src: 192.168.1.21, Dst: 192.168.1.120

Escoger Telephony->Voip Calls



Escoger el paquete y clic en el botón PLAYER



Finalmente habremos interceptado la llamada:

4.2. Pruebas

Primero se realizó las pruebas para determinar los puertos abiertos del servidor:

nmap -A 192.168.1.120

<i>Puerto</i>	<i>Servicio</i>	<i>Versión</i>	<i>Estado</i>
5060	asterisk	6.4	abierto
25	smtp	Postfix smtpd	abierto
80	http	Apache httpd	abierto
111	rcpbind	2	abierto
443	ssl/http	Apache httpd	abierto
3306	MySQL	5	abierto

En este caso se muestra los puertos que por defecto se encuentran abiertos en el servidor VOIP.

Seguidamente procedemos a realizar una prueba de fuerza bruta para averiguar la contraseña de una de las extensiones del servidor:

Svcrack -u 121 192.168.1.120 -d diccionario.txt

En donde “diccionario.txt” seria el archivo preparado previamente con las palabras y frases almacenadas para el ataque de fuerza bruta, y como resultado:

Extensión	Contraseña
108	1234

Ahora en base a la lista de los puertos abiertos podríamos determinar la contraseña del admin mediante el puerto 22 usando la herramienta hydra

hydra -l root -P diccionario.txt 192.168.1.120 -t 8 -v ssh

Lo que se obtiene es lo siguiente:

Host: 192.168.1.120 User: root Password: server2018

Como resultado de las pruebas realizadas obtenemos lo siguiente:

VULNERABILIDAD	SOLUCIÓN
Puertos innecesarios abiertos	Mediante herramienta de Test de Puertos cerrar todos los puertos innecesarios
Enumeración de dispositivos SIP habilitada.	Configurar reglas de acceso en Firewall
Permisos de escaneo de usuarios habilitado	Corregir valor por defecto en archivo sip.conf
Contraseñas obtenidas por fuerza bruta	Encriptar el archivo de configuración de seguridad del PBX
Contraseñas usuarios débiles y muy intuitivas	Utilizar software de creación de contraseñas robustas
Protocolo ssh sin protección	Establecer la protección de seguridad del protocolo en el servidor
Permiso de solicitudes concurrentes ilimitado	Establecer la protección de seguridad del protocolo en el servidor
Firewall deshabilitado	Habilitar firewall propio de Asterisk
Servicios no utilizados, habilitados	Deshabilitar servicios no usados.
Contraseña de root débil.	Utilizar software de creación de contraseñas robustas
Uso del protocolo SIP desactualizado	Cambiar al protocolo IAX

CAPITULO V

DISCUSIÓN DE RESULTADOS

5.1. Contrastación de los resultados

Después de haber realizado la aplicación y las pruebas de vulnerabilidad en el servidor VOIP se puede finalizar la investigación concluyendo que el protocolo que debe implementarse es el IAX por ser un protocolo robusto en el tema de seguridad, ya que las llamadas se encriptan cuando viajan por la red, lo que no sucede con el protocolo SIP, cabe destacar que SIP es más ligero y más fácil de implementar y ofrece compatibilidad en la mayoría de equipos y servidores, pero el resultado como pudimos ver que se pudo interceptar las llamadas, y guardarlas en formato MP3, ya cuando se migra al protocolo IAX, es casi imposible interceptar las llamadas, y en el caso que fuese posible no se oiría nada solo ruidos efecto de la misma encriptación de las llamadas.

A continuación, se adjunta una tabla en la cual se detallan algunas diferencias cruciales en el uso de los protocolos en VOIP:

	SIP	IAX	Conclusión
Tipos de Mensajes	Los mensajes son en formato de texto.	Los mensajes son en formato binario	IAX consume menos ancho de banda.
Señalización	Datos y señalización en puertos distintos.	Datos y señalización por el mismo puerto.	En SIP aparecen problemas de NAT.
Señalización	Al ir la señalización audio por puertos distintos, el audio puede ir de extremo a extremo sin pasar por el servidor SIP	Al ir la señalización y audio por el mismo puerto, el audio pasa obligatoriamente por el servidor IAX.	Consumo alto de recursos en el servidor IAX ante una gran cantidad de llamadas.

CONCLUSIONES

- ✓ Se realizo la virtualización de los entornos de red, tanto el servidor de comunicación como los clientes.
- ✓ Se llevo a cabo fase de penetración (pentesting), donde se realizaron las pruebas y los ataques correspondientes, obteniendo resultados que se dieron a conocer en la parte de pruebas y resultados.
- ✓ Se elaboro la lista de las vulnerabilidades, como también las alternativas de solución.
- ✓ Se ha documento el proceso de prueba.

REFERENCIAS BIBLOGRÁFICAS

- 3CX. (2018). 3CX. Obtenido de <https://www.3cx.es/voip-sip/central-telefonica-pbx/>
- Anaya, N. (2018). *Protocolo IAX*. Obtenido de <http://elastixtech.com/protocolo-iax/>
- Atoio. (2018). *Actualidad Informatica*. Obtenido de <http://antoniojorz.blogspot.com/2015/04/tecnicas-de-recoleccion-de-informacion.html>
- Catoira, F. (24 de julio de 2012). *ESET LiveSecurity*. Obtenido de <https://www.welivesecurity.com/la-es/2012/07/24/penetration-test-en-que-consiste/>
- DragonJar. (2018). *DragonJar*. Obtenido de <https://www.dragonjar.org/nueva-versin-de-cain-abel.xhtml>
- Informática, T. (2018). *Tecnología Informática*. Obtenido de <https://tecnologia-informatica.com/tipos-de-redes-informaticas-lan-wan-man-wlan-wman-wwman-san-pan/>
- Networks, S. (2018). *Supra Networks*. Obtenido de <https://www.supra.com.pe/blog/ataques-ciberneticos-eavesdropping-prevencion/>
- Ramírez, I. (24 de agosto de 2018). *Xakata*. Obtenido de <https://www.xataka.com/seguridad/que-es-una-conexion-vpn-para-que-sirve-y-que-ventajas-tiene>
- SegInfoSys. (30 de agosto de 2018). *SegInfoSys*. Obtenido de <https://seginfosys.com/blog/2018/08/30/analisis-de-vulnerabilidades-versus-pentesting-que-contrato/>
- seguridad, b. d. (8 de setiembre de 2017). *blog de auditoria de seguridad*. Obtenido de

<http://blogdeauditoriadeseguridad.blogspot.com/2017/09/metodologia-ptes-penetration-testing.html>

Soto, M. G. (26 de junio de 2016). *medium.com*. Obtenido de <https://medium.com/@marvin.soto/qu%C3%A9-es-el-envenenamiento-arp-o-ataque-arp-spoofing-y-c%C3%B3mo-funciona-7f1e174850f2>

Teleradio. (2018). *Teleradio*. Obtenido de <http://www.telradio.com.mx/preguntas/que-es-sip>

VOIP, T. (2018). *Telefonia VOIP*. Obtenido de <http://www.telefoniavozip.com/voip/que-es-la-telefonía-ip.htm>